

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-337863

(43)Date of publication of application : 07.12.2001

(51)Int.Cl.

G06F 12/14
G06F 3/06

(21)Application number : 2000-157954

(71)Applicant : HITACHI LTD

(22)Date of filing : 24.05.2000

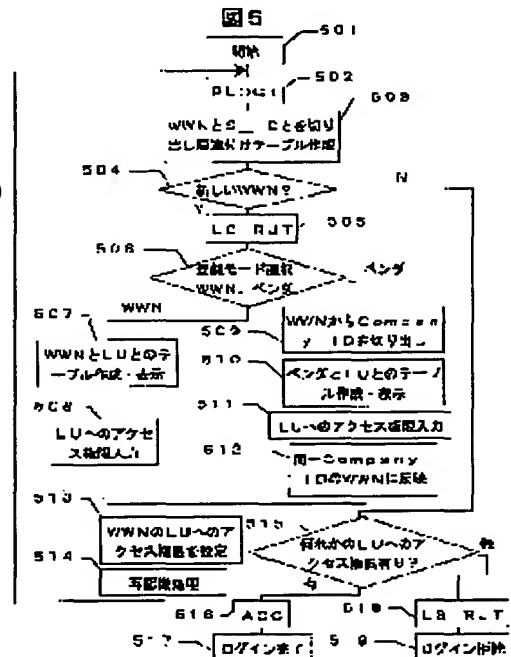
(72)Inventor : KAMANO HISAMITSU
TAKAMOTO KENICHI

(54) STORAGE CONTROLLER, STORAGE SYSTEM, AND THE METHOD FOR SETTING SECURITY FOR STORAGE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To readily authorize or inhibit an access to a storage area under the control of a storage controller, by automatically registering connected host computers.

SOLUTION: By obtaining N-Port-Name information (503) included in a login from a host computer (502) and displaying the information in the state of a table marking access permission both of a subordinate LU and of the host computer (507), an administrator can create security tables of the storage controller only by setting flag information for or against the access (508).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-337863

(P2001-337863A)

(43) 公開日 平成13年12月7日 (2001.12.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
3/06	3 0 1	3/06	3 0 1 B 5 B 0 6 5
	3 0 4		3 0 4 H

審査請求 未請求 請求項の数17 O L (全 11 頁)

(21) 出願番号 特願2000-157954(P2000-157954)

(22) 出願日 平成12年5月24日 (2000.5.24)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 鎌野 寿充

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(72) 発明者 高本 賢一

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5B017 AA01 BA06 BB06 CA01

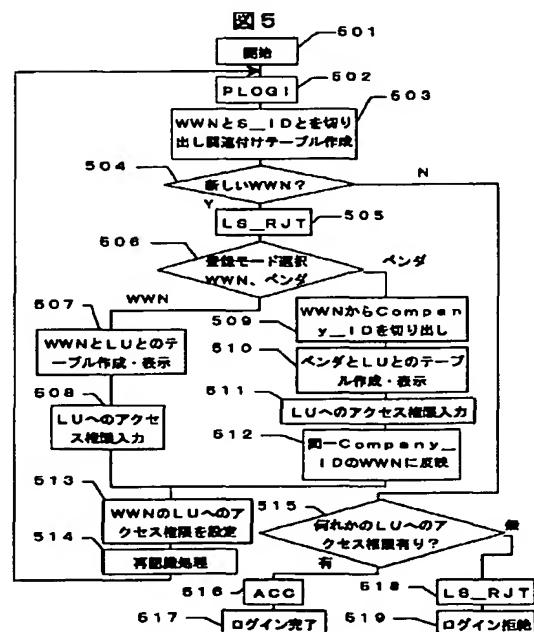
5B065 BA01 CA11 CA12 PA12 PA13

(54) 【発明の名称】 記憶制御装置及び記憶システム並びに記憶システムのセキュリティ設定方法

(57) 【要約】

【課題】 接続された上位装置を自動的に登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えることを提供する。

【解決手段】 上位装置からのログイン (502) に含まれるN_Port_Name情報を取得し (503)、配下のLUと上位装置とのアクセス権限を示すテーブルの状態管理者に表示する (507) ことにより、管理者はアクセス可否のフラグ情報設定 (508) のみで記憶制御装置のセキュリティテーブルを作成できる。



【特許請求の範囲】

【請求項 1】データを記憶する記憶領域を有する記憶装置と、

この記憶装置とのデータ転送を制御するバックエンド制御部と、前記記憶装置から読み出した情報を一時的に格納するキャッシュと、このキャッシュと上位装置との間のデータ転送を制御するフロントエンド制御部と、前記上位装置より送られてきたフレームからこの上位装置を識別する情報を入手しメモリに記憶させるプロセッサとを有する記憶制御装置と、を備えた記憶システム。

【請求項 2】データを記憶する記憶領域を有する記憶装置と、

この記憶装置の記憶領域を認識する手段と、上位装置からのログイン要求に含まれるフレームから前記上位装置を識別する情報を分離する手段と、この分離した情報を元に接続されている上位装置と前記記憶領域とを表示するモニタと、この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力するパネルと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定する手段と、を有する記憶制御装置と、を備えた記憶システム。

【請求項 3】前記上位装置を識別する情報は、N__Port__Name または World Wide Name である請求項 1 又は 2 記載の記憶システム。

【請求項 4】前記上位装置を識別する情報は、Company__ID である請求項 1 又は 2 記載の記憶システム。

【請求項 5】前記 Company__ID に対応するベンダの情報を予め記憶しておく請求項 4 記載の記憶システム。

【請求項 6】前記上位装置を識別する情報は、上位装置のプロトコル、ファイル形式または OS の何れかである請求項 1 又は 2 記載の記憶システム。

【請求項 7】前記記憶制御装置は前記上位装置とネットワークを介して接続される請求項 1 乃至 6 の何れか記載の記憶システム。

【請求項 8】前記記憶制御装置は異なったプロトコル及び／または異なったファイルシステムを持つ複数の前記上位装置と接続される請求項 1 乃至 6 の何れか記載の記憶システム。

【請求項 9】配下の記憶装置とのデータ転送を制御するバックエンド制御部と、前記記憶装置から読み出した情報を一時的に格納するキャッシュと、このキャッシュと上位装置との間のデータ転送を制御するフロントエンド制御部と、前記上位装置より送られてきたフレームからこの上位装置を識別する情報を入手しメモリに記憶させるプロセッサとを有する記憶制御装置。

【請求項 10】配下の記憶領域を認識する手段と、上位装置からのログイン要求に含まれるフレームから前記上位装置を識別する情報を分離する手段と、この分離した

情報を元に接続されている上位装置と前記記憶領域とを表示するモニタと、この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力するパネルと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定する手段と、を有する記憶制御装置。

【請求項 11】上位装置を識別する情報を含んだフレームを受信するステップと、前記フレームから前記情報を分離して記憶するステップと、

10 記憶制御装置配下の記憶領域を認識するステップと、前記分離した情報を元に前記上位装置と前記記憶領域とのテーブルを作成するステップと、前記テーブルに前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項 12】ログイン要求を受信するステップと、前記ログイン要求に含まれるフレームから上位装置を識別する情報を分離するステップと、記憶制御装置配下の記憶領域を認識するステップと、

20 前記分離した情報を元に接続されている上位装置と前記記憶領域とを表示するステップと、この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定するステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項 13】前記上位装置を識別する情報は、N__Port__Name、World Wide Name、Company__ID の何れかである請求項 12 記載のセキュリティ設定方法。

【請求項 14】PLOGI を受信するステップと、この PLOGI に含まれるフレームから N__Port__Name 又は World Wide Name を分離するステップと、

35 この N__Port__Name 又は World Wide Name と前記 PLOGI に含まれる S__ID とを関連つけるテーブルを作成するステップと、前記 N__Port__Name 又は World Wide Name が予め記憶されているものか判断するステップと、

40 前記判断により予め記憶されたものでない場合に、記憶制御装置配下の記憶領域を認識するステップと、前記分離した N__Port__Name 又は World Wide Name を元に接続されている上位装置と前記記憶領域とを表示するステップと、

45 この表示に基づき前記上位装置がアクセス可能な前記記憶領域を入力させるステップと、この入力に基づき、前記上位装置の前記記憶領域に対するアクセス権限を設定するステップと、

50 前記上位装置に再度 PLOGI を発信させるステップ

と、を備えた記憶システムのセキュリティ設定方法。

【請求項 15】前記アクセス可能な前記記憶領域の入力は、リードコマンドのアクセスとライトコマンドのアクセスとを別個に行なう請求項 11 乃至 14 の何れか記載の記憶システムのセキュリティ設定方法。

【請求項 16】ログイン要求を受信するステップと、前記ログイン要求に含まれるフレームから World Wide Name を分離するステップと、この World Wide Name から更に Company ID を分離するステップと、同一 Company ID と記憶領域とのアクセス権限が既に登録されている場合に、前記アクセス権限を前記ログイン要求を行なった上位装置のアクセス権限とするステップと、を備えた記憶システムのセキュリティ設定方法。

【請求項 17】前記アクセス権限を、前記上位装置に転送するステップを有する請求項 11 乃至 16 の何れか記載のセキュリティ設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置間での不正アクセス防止を行なうセキュリティ設定に関する。具体的には上位装置（ホストコンピュータ）と記憶制御装置（記憶システム）との間にネットワークを構成したコンピュータシステムにおいて、記憶制御装置配下にある記憶領域へのアクセス要求があった際の、不正アクセス防止を行う記憶システム及びこの記憶システムを含むコンピュータシステムに関連する。

【0002】

【従来の技術】ANSI X3T11 で標準化されたファイバチャネルプロトコルでは、多数の装置が接続可能であり、かつ SCSI、ESCON、TCP/IP 等多種のプロトコルを同時に運用可能な利点がある。しかし、異種プロトコルのため異なるファイルシステムによるアクセスによって記憶装置のデータが破壊される恐れが生じる等の問題に対し、セキュリティ確保等の対策を行なう必要性が発生する。

【0003】このセキュリティ確保としては、特開平 10-333839 号公報に記載のように、記憶制御装置配下の記憶領域に対するアクセスを許可するために、上位装置を一意に識別する情報と記憶領域へのアクセス可否を表すテーブルを記憶制御装置内に設定しておき、アクセス時にこのテーブルを比較することで、アクセス可能な上位装置以外からのアクセスを拒絶することで不正アクセスを防止する技術がある。

【0004】この識別情報とはホストバスアダプタ毎に固有な N_Port_Name 或いは WWN (World Wide Name) と呼ばれる 48 ビットの数字の羅列である。上位装置の識別情報を記憶制御装置内に予め登録しておくことにより、上位装置は記憶制御装置配下にある記憶

装置内の記憶領域にアクセスすることができる。

【0005】

【発明が解決しようとする課題】上位装置の識別情報を記憶制御装置内に予め登録しておくため、ユーザ或いは管理者は、上位装置と LAN で接続されたマネージャ等により、上位装置に固有な 8 バイトの領域を持ち 48 ビットの数字で表される N_Port_Name を調査する。そしてこの数字を控えるなどした後、自らの手で記憶制御装置へ登録する必要がある。そのため、この登録の際に上位装置の N_Port_Name を入力ミスし、意図した上位装置が記憶領域にアクセス出来なかったり、逆に意図しない上位装置が記憶領域にアクセスしデータを破壊してしまう恐れがある。

【0006】また、多数台の上位装置に対するアクセス可否を登録する場合、非常に時間を要することになる。従って、識別情報の取得および設定に関して、簡易に扱うことが望まれる。

【0007】本発明の目的は、接続された上位装置を一意に識別する情報を取得し、自動的に記憶制御装置内に登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えるシステムを提供することにある。

【0008】

【課題を解決するための手段】上記目的を解決するために本発明は、はじめに上位装置から送信されてくるフレーム内に格納された上位装置を識別する情報を取得し、記憶制御装置内に登録し、管理者がアクセスを許可する上位装置についてアクセスを許可するフラグ情報の設定を変更する。

【0009】

【発明の実施の形態】以下、本発明の実施例について図面を用いて説明する。

【0010】まず、本発明の対象となる記憶システムとして記憶制御装置と磁気ディスク装置、この記憶システムと上位装置との間にファイバチャネルを用いて構築したネットワークを用いて構成したコンピュータシステム、いわゆる SAN (Storage Area Network) 環境におけるコンピュータシステムについて説明する。

【0011】ファイバチャネルとは、独自のコマンドセットを持たないシリアル転送方式をもつプロトコルであり、情報を非同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして独自のコマンドセットを持たないかわりに、物理転送方式を、SCSI、ESCON といったコマンドセットの運搬路として使用することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【0012】図 1 は、本発明のコンピュータシステムのハードウェア構成図である。図 1 において、上位装置 10、20、30 はデータ処理を行う中央処理装置として

の役割を果たす。複数の磁気ディスクドライブ 50 は、記憶制御装置 40 の配下にアレイ状に接続される記憶媒体からなる記憶装置である。記憶制御装置 40 はこの磁気ディスクドライブ 50 の制御を行なうディスクアレイ装置である。

【0013】記憶制御装置 40 は、上位装置 10、20、30 との間のファイバチャネルプロトコルを制御するフロントエンド制御部（チャネルアダプタ）41、記憶制御装置 40 全体を制御するマイクロプロセッサ 42、記憶制御装置 40 の動作を制御するマイクロプログラム及び制御用データ並びに後述する各テーブルを格納する不揮発の制御メモリ 43、データを一時的に格納（バッファリング）しておくキャッシュ 45、このキャッシュへ 45 のデータの読み書きを制御するキャッシュ制御部 44、磁気ディスクドライブ 50 との間に使用されているプロトコルを制御し、磁気ディスクドライブ 50 とのデータデータ転送を制御するバックエンド制御部（ディスクアダプタ）46、情報設定を行うパネル 47 から構成される。

【0014】磁気ディスクドライブ 50 は、論理的に分割した区画に分けられる。SCSI のプロトコルでは、この区画を LU（Logical Unit）といい、その領域は、各々、LUN（Logical Unit Number）という番号を持つ。本実施の形態では、LUN0 番の LU である LU0（51）と、LUN1 番の LU である LU1（52）との 2 つの領域を有する場合を示している。

【0015】上位装置 10、20、30 と記憶制御装置 40 は、ファイバチャネル 60 をインタフェースとし、ファブリック（Fabric）というスイッチ装置を介して接続されている。

【0016】図 1 のシステムの動作を、上位装置 10 が記憶制御装置 40 を経由してディスクドライブ 50 内に構成された LU0（51）とデータ転送を行う場合を例にとって説明する。上位装置 10 が記憶制御装置 40 にログインし、その後 LU0（51）に対してアクセス要求（I/O 要求）を出すと、その要求を受けたフロントエンド制御部 41 はマイクロプロセッサ 42 に割込み要求を行う。マイクロプロセッサ 42 は、上位装置 10 からのコマンド情報や上位装置 10 を認識する情報を制御メモリ 43 に格納する。上位装置 10 が LU0（51）に対してアクセスが許可されている場合は、コマンド情報を確認する。

【0017】確認したコマンドがリードコマンドであった場合、マイクロプロセッサ 42 は、アクセス要求のあったデータブロックがキャッシュ 45 にあるか否かを判断する。該当データがある場合にはそのデータを上位装置 10 に転送し、上位装置 10 に完了報告を行う。該当データが無い場合には、バックエンド制御部 46 を使って、アクセス要求のデータブロックを LU0（51）から読み出し、キャッシュ制御部 44 を使ってキャッシュ

45 ヘデータを格納する。次にマイクロプロセッサ 42 は、フロントエンド制御部 41 を使って、キャッシュ 45 に格納したデータを上位装置 10 に転送し、上位装置 10 に完了報告を行う。

05 【0018】確認したコマンドがライトコマンドであった場合、マイクロプロセッサ 42 は、ライト要求のデータブロックをキャッシュ 45 に格納し、上位装置 10 に完了報告を行う。その後、キャッシュ制御部 44 を使って LU0（51）ヘデータを転送し書き込みを終了する。

10 【0019】ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図 2 を用いて説明する。図 2 に示すように、フレーム 70 はスタートオブフレーム SOF（Start Of Frame）71、リンク動作の制御やフレームの特徴づけを行う 24 バイトのフレームヘッダ 72、実際に転送される目的となるデータ部分であるデータフィールド 73、4 バイトのサイクリックリダンダンシチェック CRC（Cyclic Redundancy Check）74、およびエンドオブフレーム EOF（End Of Frame）75 で構成される。データフィールド 73 は 0 ～ 2112 バイトの間で可変である。

15 【0020】SOF 71 は、フレームの先頭に置く 4 バイトの識別子である。EOF 75 は、フレームの最後につける 4 バイトの識別子で、SOF 71 と EOF 75 によりフレームの境界を示す。ファイバチャネルではフレームがないときはアイドル（idle）という信号が流れている。フレームヘッダ 72 のフォーマット 80 を図 3 に示す。

20 【0021】フレームヘッダの構造について説明する。0 ワードの 23-0 ビット領域にあたるデスティネーションアイデンティファイ D_ID（Destination ID）81 はフレーム受け取り側のアドレス識別子である。また、1 ワードの 23-0 ビット領域にあたるソースアイデンティファイ S_ID 82 は、フレームの送信先ポートを識別する 3 バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。そして上位装置を動的に一意に識別できる情報であり、PLOGI 時（後述）に上位装置より報告される値である。この S_ID 82 はシステム立ち上げ毎等に動的に変動する値であり、FC-PH（Fibre Channel Physical and Signaling Interface：ファイバチャネルの米国標準規格）ではファブリックによって初期化手続き時に割り当てられることになっている。割り当てられる値は、それぞれのポートが持つ N_Port_Name、Node_Name に依存する。

45 【0022】フレームは機能に基づいてデータフレームと制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。一方、リンク制御フレームは、一般に、フ

ム配信の成功あるいは不成功を示すのに使われる。フレームを1個受信したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【0023】次に、「シーケンス」について説明する。ファイバチャネルにおけるシーケンスは、あるN__Portから別のN__Portへ、一方向に転送されるデータフレームの集まりのことをいい、SCSIのフェーズに相当する。シーケンスの集まりをエクステンジと呼ぶ。例えば、コマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクステンジとなる。このように、エクステンジはSCSIのI/Oに相当する。ファイバチャネルインタフェースでは、上位装置がデバイスに対して、通信パラメータを含むポートログインPLOGI（N__Port Login）コマンドのフレームを送り、デバイスがこれを受け付けることで通信が可能となる。これをログインという。

【0024】何れかの上位装置から記憶制御装置40への通信要求であるPLOGIフレームの構造について説明する。データフィールド73の詳細構造において、先頭から20バイト目～27バイト目（5～6ワード目）までの8バイトの領域がN__Port__Nameを格納する領域であり、先頭から28バイト目～35バイト目（7～8ワード目）までの8バイトの領域がNode__Nameを格納する領域である。

【0025】デバイスは、要求を受け付ける場合はアクセプトACC（Accept）と呼ばれるフレームを、要求を拒絶する場合はリンクサービスリジェクトLS__RJT（LinkService Reject）フレームを、それぞれ、上位装置に送る。

【0026】図4にログインシーケンス100を示す。ログイン要求元である上位装置は、PLOGIフレームをログイン要求先であるデバイスの記憶制御装置40へ送信する。このPLOGIフレームには、そのフレームヘッダ72内にはS__ID82及びその他の情報が、データ・フィールド73内にログイン要求元のN__Port__Name、Node__Nameが含まれている。

【0027】記憶制御装置40では、このフレームに含まれている情報を取り出し、ログインを受諾する場合はACCフレームをログイン要求元に対して送信する。ログインを拒絶する場合は、PLOGIフレームに対して、記憶制御装置40はLS__RJTと呼ばれるフレームを上位装置に対して送信する。

【0028】次に、本発明によるセキュリティ情報の取得ならびに自動登録について図5を用いて説明する。

【0029】周辺装置である記憶制御装置40等を先に立ち上げた後で、上位装置10、20、30を立ち上げる（ステップ501）。各上位装置は、各々のN__Po

rt__Name情報を格納したログイン要求フレームであるPLOGIフレームを発行する。

【0030】上位装置が追加された場合には、PLOGIの代わりにFLOGI（ファブリックログイン）の処理がスイッチ装置との間で行われた後、スイッチ装置は接続されたデバイスすべてに対して状態に変化が生じたことを示すRSCN（Registered State Change Notification）を通知する。そして追加された上位装置に対してGPN__ID（Get Port Name）を送信し、N__Port__Name情報を要求する。（ステップ502）。記憶制御装置40のマイクロプロセッサ42は、フロントエンド制御部41のポートP0を経由してN__Port__Nameの含まれたフレームを受領する。尚図面においてはN__Port__Nameの代わりにWWN（World Wide Name）を使用している。WWNはN__Port__Name同様、各装置固有の8バイトの値であり、ポート毎に固有なPort__Nameと、ノード毎に固有なNode__Nameとの和集合である。

【0031】後述する実際のI/O要求時（Inquiry）のフレームには、N__Port__Nameが付加されておらず、立ち上げ毎に値が変化するS__IDのみが付加される。そこでマイクロプロセッサ42は、PLOGIのフレームヘッダからS__IDを、データ・フィールドからN__Port__Nameを切り出し、InquiryにS__IDからN__Port__Nameを引き出せるように関連付けた、図6（a）に示す様な上位装置情報テーブル200を作成して制御メモリ43内に格納しておく（ステップ503）。

【0032】次に、マイクロプロセッサ42は、ステップ503にて切り出したWWNが制御メモリ43内の上位装置情報テーブル200に登録されているWWNと一致するか否かを確認する（ステップ504）。

【0033】新規のWWNだった場合には、セキュリティテーブルへの登録が行なわれていないために、そのPLOGIを発行した上位装置に接続を拒絶するリジェクトパラメータをいれたLS__RJTを応答し、拒絶を行なう。（ステップ505）。そして新しい上位装置が接続されたものと認識し、パネルの表示部に新しい上位装置が接続された旨を表示し、セキュリティテーブルへの登録を行なうためのモード選択を管理者に促す。選択できるモードとしては、WWNそのものを使用して登録するモードと、WWN内に含まれるCompany__IDを用いて登録するモードとを備える（ステップ506）。尚、新しい上位装置が接続された旨は、画面の点滅や音声による案内等、管理者が認識しやすい表示の仕方とする。

【0034】Company__IDについて説明する。N__Port__Name8バイトは、その60～63ビットの4ビットエリアに識別フィールドを、36～59ビットの24ビットエリアにCompany__IDを、

0～35ビットの36ビットエリアにVS_ID (Vendor Specific Identifier) を含んで構成されている。ここでCompany_IDは、各ベンダ毎にユニークな値が割り振られている。つまり、同じベンダは同じ値を備えている。

【0035】異なるプロトコルや異なるファイルシステムを持つ上位装置からのI/Oによるデータ破壊を防止するためのセキュリティでは、同じベンダの上位装置がアクセスできるデバイスは同一である場合が多い。そのため、ベンダ毎のセキュリティを設定しても問題が多く、複数台まとめてアクセス可否を設定出来るので、より簡易にセキュリティテーブルの作成が行なえる。

【0036】管理者がWWN毎（複数の上位装置を登録する場合でも1台毎）の登録を選択した場合、マイクロプロセッサ42は、装置立ち上げ時等セキュリティテーブルが全く作成されていない場合には、記憶制御装置40配下の記憶領域であるLUを認識する。そして図6

(b) に示すような上位装置とLUとのセキュリティテーブル201を作成する。上位装置の追加時や再立ち上げ時等、前もってセキュリティテーブル201が存在する場合には、セキュリティテーブル201に新しいWWNに相当する上位装置を追加し新しいセキュリティテーブルを作成する。

【0037】そしてこのセキュリティテーブル201をパネル47の表示部に表示する（ステップ507）。管理者は、パネル47を用いてこのテーブルに上位装置のアクセス可否のみを入力する（ステップ508）。

【0038】入力の仕方の一例を図7に示す。図7はパネル47を示している。表示部471には、自動登録された上位装置（この場合にはHost A, Host Bは既に登録されている上位装置であり、Host Cが新しく登録された上位装置とする）が表示される。キー部472の矢印キーを押すことによってHost Cを選択すると、LUアクセス許可・抑止フラグ情報の設定変更が可能となる。ここで管理者はEnableを選択することでアクセスを許可できる。このLUアクセス許可・抑止フラグ情報はデフォルトでは、Disableとしておく方が良い。キー部472には数字キーも備えることで従来の様にWWNを手入力することも出来る。図7では簡単のため、LU（記憶領域）が一つの場合の例を示している。

【0039】管理者がベンダ毎の登録を選択した場合、マイクロプロセッサ42は、WWNからCompany_IDを切り出す（ステップ509）。そしてこのCompany_IDを用いて図6(c) に示すようなベンダとLUとのアクセス可否テーブル202を（ステップ507）と同様にして作成し表示する（ステップ510）。管理者は、このテーブルにパネル47を用いて上位装置のアクセス可否のみを入力する（ステップ511）。

【0040】セキュリティテーブル201は上位装置（WWN）とLUとの対応を表しているので、ステップ511にて作成したアクセス可否テーブル202を参考にして、各Company_IDを有する上位装置（WWN）のアクセス可否入力を自動的に行ない、ステップ507の代替とする（ステップ512）。

【0041】以上の入力を元にして、セキュリティテーブル201を完成させ、設定更新する（ステップ513）。

【0042】この様にして新しいセキュリティテーブル201に更新された後、マイクロプロセッサ42は上位装置にGPN_ID (Get_Port_Name) を発行することで、再度上位装置にPLOGIを発行させる（ステップ514）。

【0043】今度は新しいWWNではないのでステップ504においてNが選択されステップ515に進む。

【0044】ステップ504において、WWNが既知の場合には、ログイン続行し、このWWNが記憶制御装置40にログイン可能か否かを判断する。そのために、セキュリティテーブル201を参照して、このWWNが記憶制御装置40配下の何れかのLU（図1の場合にはLU0かLU1）にアクセス権限が有るか否かを判断する（ステップ515）。

【0045】アクセス権限が設定されている上位装置には、ACCを返し（ステップ516）、ログインを完了する（ステップ517）。

【0046】アクセス権限がない上位装置には、LS_RJTを返し（ステップ518）、ログインを拒絶する（ステップ519）。

【0047】ここで、初期システム立ち上げ時の様に、複数台の上位装置が新しく接続された場合、どの上位装置がどのWWNであるかということを管理者は認識できない。そのため、ステップ506において、WWN毎に登録を選択する場合には、別途システムに接続されたSANマネージャ等からどの上位装置がどのWWNを備えているかをチェックしておくことによって、管理者はアクセス権限の有無を入力するのみでセキュリティテーブル201を作成する事が出来る。

【0048】ここで、SANマネージャ装置について図12を用いて説明する。上位装置10, 20, 30ならびに記憶制御装置40はファイバチャネルFabric 60とは別にローカルエリアネットワーク（LAN）61で接続されている。このLAN61にはSANマネージャ装置90やファイバチャネルFabric 60も接続されている。SANマネージャ装置90はPCやWSであり、LAN61経由で上位装置10, 20, 30や記憶制御装置40ならびにファイバチャネルFabric 60からSANのシステム構成を表す情報を取得する。

【0049】また、ステップ506において、ベンダ毎

の登録モードを選択した場合に備えて、予め制御メモリ内に各ベンダの Company__ID を記憶しておくことで、新しい WWN が何れのベンダの上位装置かを知ることが出来る。よって、初期設定時においても管理者はモード選択を行なうのみでアクセス権限の有無を入力することもなく、セキュリティテーブル 201 を作成する事が出来る。

【0050】次に、Inquiry コマンド実行について図 8 を用いて説明する。Inquiry コマンドとは、I/O プロセスを開始しようとする場合に先立ち、プロセスの対象となる論理デバイスに対して、その実装状態を問い合わせるコマンドである。具体的には、上位装置から記憶制御装置 40 配下の記憶領域 LU へのアクセス要求に先立つ情報問い合わせ要求のことである。本コマンドは SCSI では必ずサポートされている標準コマンドである。

【0051】フレームヘッダ 80 の詳細構造において、LU にアクセスしようとする上位装置は、アクセスしようとする LU をもつ記憶制御装置 40 に対し、Inquiry コマンドを含むフレームを送信する（ステップ 801）。このフレームには、PLOGI で割り当てられた、上位装置の S__ID 82 と、問い合わせを行う LU の識別子である LUN が含まれている。

【0052】そして Inquiry が発行されて I/O を行なう際には、Inquiry フレームより S__ID 82 を切り出し（ステップ 802）、N__Port__Name と S__ID 82 とを関連付けたテーブルから S__ID 82 に対応する N__Port__Name を求める事で、Inquiry が何れの上位装置によって発行されたものかを判定する（ステップ 803）。

【0053】そして判定された上位装置が I/O を行なう LU に対してアクセス権限があるか否かをセキュリティテーブル 201 により判定し（ステップ 804）、権限がある場合にはアクセスを受付けるために Inquiry を発行した上位装置に対して ACC を返し（ステップ 805）、I/O 処理を行なう（ステップ 806）。権限がない場合には LS__RJT を上位装置に返し（ステップ 807）、I/O 要求を拒絶する（ステップ 808）。

【0054】以上のように、I/O 処理か I/O 要求拒絶を行い Inquiry は終了する（ステップ 809）。

【0055】次に、図 9 を用いて、上位装置の登録のみならず、セキュリティ設定までも自動登録するモードを備えた機能を有する実施例を説明する。

【0056】ステップ 901 から 909 までは、図 5 に示したステップ 501 から 509 と同一なので説明は省略する。

【0057】ステップ 909 において Company__ID を切り出した後、ユーザはセキュリティ登録を手動

で行なうか自動で行なうか選択する（ステップ 910）。

【0058】手動を選択した場合、ステップ 911 と 912 とは、図 5 に示したステップ 510 と 511 と同一なので説明は省略する。

【0059】自動を選択した場合、マイクロプロセッサ 42 は、セキュリティテーブル 200 に登録されている上位装置の中に、新しい WWN の Company__ID と同一のものが有るか否かを検索する。（ステップ 913）。

【0060】無い場合には、セキュリティ自動設定は行なう事が出来ないの、手動設定と同様にステップ 911 へ進む。同一 Company__ID がある場合には、その Company__ID のセキュリティ設定をコピーすることで当該上位装置に対するアクセス可否設定入力を省く（ステップ 914）。

【0061】以上のようにして、ベンダ毎のセキュリティテーブルを作成した後のステップ 915 以降は、図 5 のステップ 613 以降と同様であるので説明は省略する。

【0062】次に稼動しているコンピュータシステムにおいて、障害等により上位装置の一時停止、或いはホストバスアダプタを交換する場合について、図 10 を用いて説明する。

【0063】ある上位装置がシステムから抜かれた（ステップ 1001）とき、すなわち上位装置に接続されたケーブルをスイッチ装置から抜いたとき、ファイバチャネル 60 のスイッチ装置（図示せず）は、接続されたデバイスすべてに対して状態に変化が生じたことを示す RSCN を通知する（ステップ 1002）。この通知を受信した記憶制御装置 40 は、アクセプト（ACC）フレームを送信する（ステップ 1003）。記憶制御装置 40 は、既にログイン中の上位装置の中に RSCN で通知のあった上位装置があるかを確認する（ステップ 1004）。あった場合には、その上位装置に対して GPN__ID を送信する（ステップ 1005）。

【0064】上位装置は接続を外されたため、GPN__ID に対する応答をすることができないので、記憶制御装置 40 はアクセプト（FS_ACC）を受信することができない（ステップ 1006）。そこで記憶制御装置 40 でこの上位装置に対して内部的にログアウト処理を実施する。そしてセキュリティテーブル 200 のアクセス許可・抑止フラグ情報を、Disable に変更し、アクセス抑止する（ステップ 1007）。ホストバスアダプタを交換後、スイッチ装置に接続し直すときは、N__Port__Name 情報が変更になるため、上位装置新設／追加に関する実施例と同様となる。

【0065】ここで、ステップ 1007 においてセキュリティテーブル 200 のアクセス許可・抑止フラグ情報の変更を行なわないように設定しておけば、上位装置の

停止が一時的であったり、修理を完了して復帰した場合には、セキュリティテーブル200の再設定を行なうことなく、停止以前と同じ記憶領域にアクセスする事が出来る。ホストバスアダプタ交換処理は同じポートにおけるケーブルの挿抜処理を行うため、“障害等によるホストアダプタ交換と判断する”モードにしておく、管理者がパネル47からアクセスを許可しなくても、アクセスできるように自動設定される(ステップ512)。逆に、“アクセス許可・抑止を行う”モードにしておけば、上位装置追加に関する実施例と同じ処理にて、追加処理がなされる。

【0066】次に図11を用いてLUセキュリティ変更について説明する。パネル47を用いてセキュリティテーブルの変更を開始する(ステップ1101)。最初は変更モードをWWN毎かベンダ毎かを選択する(ステップ1102)。

【0067】WWN毎を選択した場合には、マイクロプロセッサ42は、パネル47の表示部471に設定されている上位装置の一覧を示す(ステップ1103)。そして管理者は、キー部472を用いて変更する上位装置のアクセス可否を変更する(ステップ1104)。

【0068】ベンダ毎を選択した場合には、マイクロプロセッサ42は、上位装置情報テーブル200のWWNからCompany_IDを切り出し、ベンダ毎のアクセス可否テーブル202作成する(ステップ1105)。そしてこのベンダ毎のアクセス可否テーブル202をパネル47の表示部471に示す(ステップ1106)。管理者は、キー部472を用いて変更するベンダのアクセス可否を変更する(ステップ1107)。その結果に基づきマイクロプロセッサ42は、変更したベンダのCompany_IDを持つWWNを検索し、ステップ1104と同じ結果となるようにする(ステップ1108)。

【0069】そしてマイクロプロセッサ42は、セキュリティテーブル201を変更する(ステップ1109)。そして上位装置に再認識処理を行わせるコマンドを発信し(ステップ1110)、上位装置はこのコマンドに対してPLOGIを発信することでログインを行なう(ステップ1111)。尚、アクセス可能だった上位装置をアクセス不可にするためには、再認識処理の前に記憶制御装置側40で、内部的にアクセス不可にする上位装置をログアウトさせておく。

【0070】上記の3例では、記憶制御装置40のフロントエンド制御部41のLU単位でのアクセス許可・抑止を行っているが、LU毎ではなく、記憶制御装置40毎で設定することも可能であり、その場合にはセキュリティテーブル201のアクセス先がLUではなく記憶制御装置40の形式となる。また、フロントエンド制御部41が複数のポートを持つ場合には、ポート毎に上位装置のアクセス権限を設定する事で、上位装置の競合を避

けたり優先度をつける事が可能となる。

【0071】また、セキュリティテーブル201を記憶制御装置40で作成後に上位装置に転送し、上位装置自身がPLOGIやInquiryを発信する前にアクセス権限が有るか否かを判断することによってセキュリティシステムを構築してもよい。この場合には、上位装置は各記憶制御装置から送られてきたセキュリティテーブルから自身のアクセス権限のところのみを選択して記憶しておけばよい。同様に、上位装置と記憶制御装置の間に位置するスイッチ或いはSANマネージャ内にセキュリティテーブルを設けてもよい。この様にすることで、ファイバチャネルを転送されるコマンドや、記憶制御装置が処理するコマンドを減少させることが出来、I/O処理をより効率的に行なう事が出来る。

【0072】また、異種プロトコルや異なるファイルシステム、異なるOSからのアクセスによるデータ破壊は、通常はデータライト時にのみ発生するものであり、データリードに関しては他のプロトコルや異なるファイルシステムを持つ上位装置からも行なえた方が便利なが多い。よって、図5のステップ507やステップ508の様に、ユーザにアクセス権限を入力させる際にリードアクセスとライトアクセスとを別々に設定させることで、読み出しのみは許可する記憶領域を備えたり、書き込みのみアクセス権限を設けさせるような設定として読み出しは自由に行なえるようにしてもよい。

【0073】また、同一ベンダが複数のファイル形式の上位装置を製造していることもある。その場合にCompany_IDを使用すると、本来のセキュリティを達成することが出来なくなる恐れがある。そのような場合には、Company_IDにOSやファイル形式等を識別しているコードの部分を加えて、先の実施例で説明したCompany_IDの代わりとすることで対応できる。

【0074】また、上位措置を識別する際にN_Port_Nameを用いず、PLOGIから上位装置のプロトコルやファイル形式、OSを識別することにより、これらの識別情報をCompany_ID代わりとすることで、同じファイル形式の上位装置には同一のアクセス権限を与えるような設定とすることが出来る。

【0075】尚、上記実施例においては説明を簡単にするために記憶制御装置は1台、LUは2つとしたが、複数台の記憶制御装置からなるシステムでも、LU数が3以上でのシステムであった場合、より本発明を適用する事によりセキュリティ設定を簡易化する事が出来るのは言うまでもない。また、記憶領域としてLU単位でなく、論理ボリューム単位、RAIDグループ単位、論理的に区分された単位ではない物理領域或いは物理ボリュームの単位でも設定可能である。また、記憶装置や記憶制御装置が複数台有るものの、論理的には一つの記憶装置や記憶制御装置である場合のように、上位装置、記憶

制御装置、記憶装置が複数台という場合には、論理的に複数及び物理的に複数の何れの意味をも含むものである。

【0076】また、記憶媒体として磁気ディスクの他に、光ディスクや光磁気ディスク、媒体形状としてはディスク以外にテープ等でも良いし、対象となる技術分野も上位装置と記憶制御装置との間に限らず、アクセス制限を設ける必要の生じる情報処理装置間等に適用できる事はもちろんである。

【0077】

【発明の効果】以上述べたように、本発明によって、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、記憶制御装置配下にある1つ以上の記憶領域、から構成されるコンピュータシステムにおいて、接続された上位装置を一意に識別する情報を自動的に取得・登録することにより、簡易に記憶制御装置配下にある記憶領域へのアクセスの許可・抑止を行えることができ、管理上の負担を減少させることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態を示すハードウェア構成図である。

【図2】フレームのフォーマットを示す図である。

【図3】フレームヘッダの詳細を示す図である。

【図4】上位装置とデバイス間のログイン時のシーケンス図である。

【図5】ログインとセキュリティテーブル登録・設定とのフローチャートである。

【図6】セキュリティテーブルの一例を示す図である。

【図7】セキュリティ情報登録時の表示部の一例を示す図である。

【図8】Inquiryコマンドのフローチャートである。

05 【図9】セキュリティテーブル自動設定モードを有するフローチャートである。

【図10】デバイス一時停止の際の処理を示すフローチャートである。

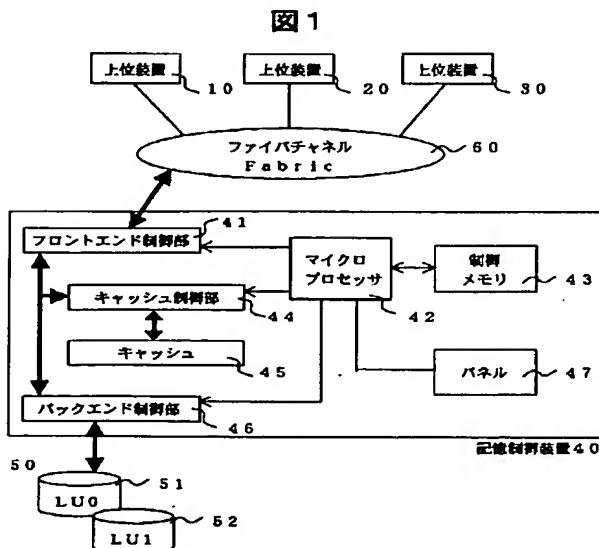
10 【図11】セキュリティテーブル変更と再ログインのフローチャートである。

【図12】SANマネージャを示す図である。

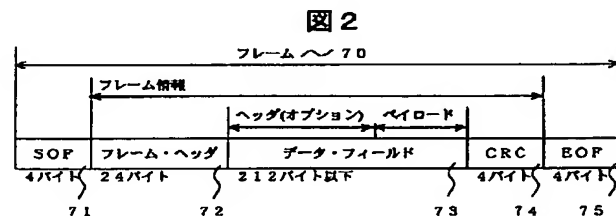
【符号の説明】

10、20、30…上位装置、40…記憶制御装置、41…フロントエンド制御部、42…マイクロプロセッサ、43…制御メモリ、44…キャッシュ制御部、45…キャッシュ、46…バックエンド制御部、47…パネル、50…磁気ディスクドライブ、51…LU0、52…LU1、60…ファイバチャネル、61…ローカルエリアネットワーク、70…フレーム、71…スタートオブフレーム、72…フレームヘッダ、73…データフィールド、74…サイクリック・リダンダンシチェック、75…エンドオブフレーム、80…フレームヘッダ、81…デスティネーションアイデンティファイア、82…ソースアイデンティファイア、90…SANマネージャ装置、200…上位装置情報テーブル、201…セキュリティテーブル、202…ベンダ毎のアクセス可否テーブル、471…表示部、472…キー部。

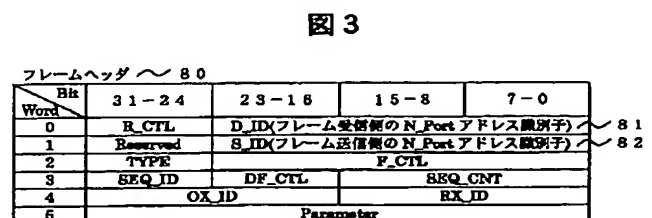
【図1】



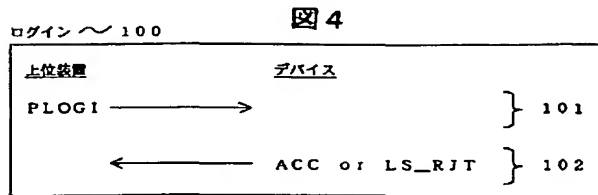
【図2】



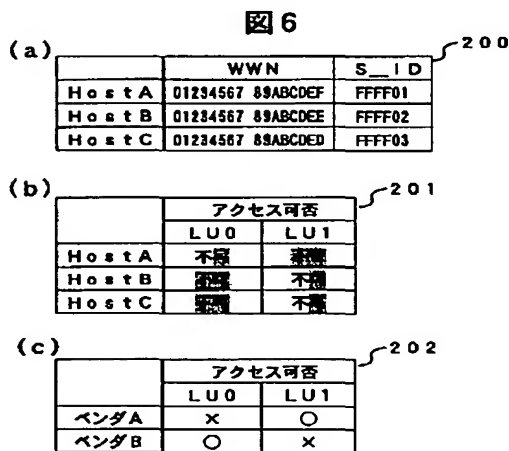
【図3】



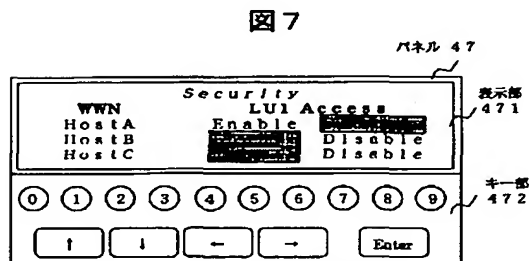
【図4】



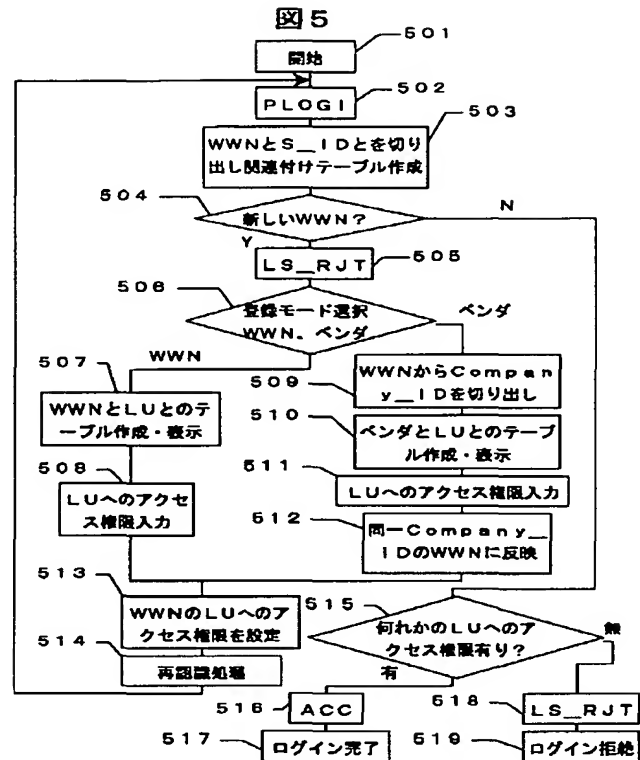
【図6】



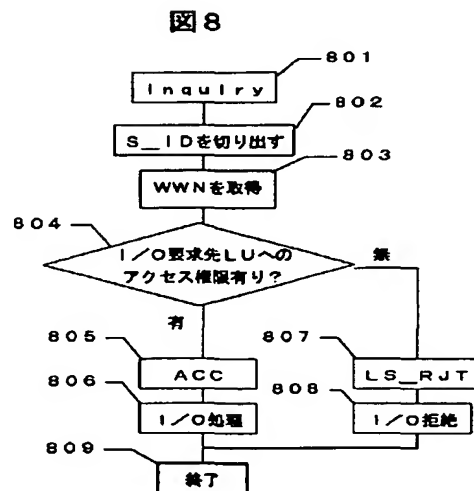
【図7】



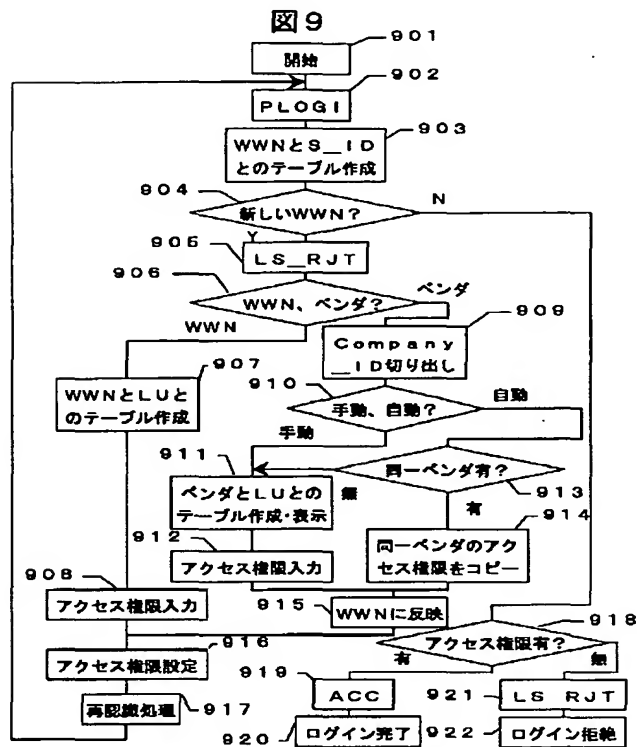
【図5】



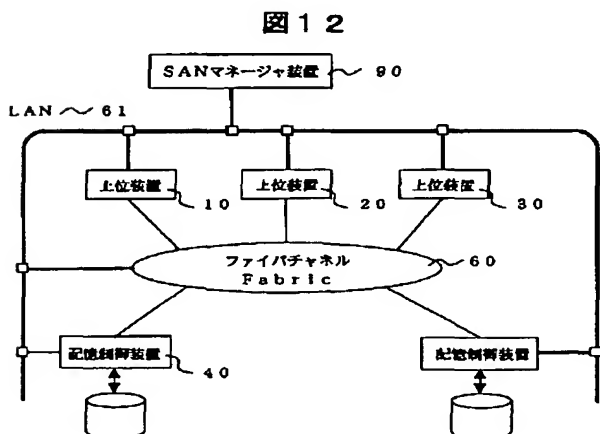
【図8】



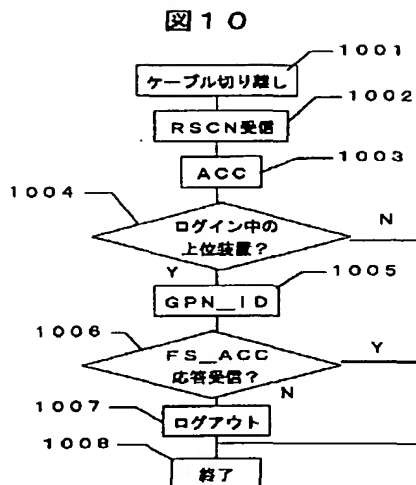
【図9】



【図12】



【図10】



【図11】

